## AMENDMENTS TO CLAIMS

Claim 1 (currently amended): A method for remote administration of at least one smart card via a communication network, the method comprising:

B1

associating said at least one smart card with a remote administrator by storing administrator identification information of the remote administrator in said at least one smart card;

inserting said at least one smart card in at least one user unit;

employing the administrator identification information stored in said at least one smart card to identify the remote administrator associated with said at least one smart card; and

establishing communication between the at least one smart card and the remote administrator via the communication network in accordance with the administrator identification information,

wherein said establishing comprises:

identifying a local administrator other than the remote administrator, the local administrator being positioned in the communication network in proximity to said at least one user unit; and

determining the local administrator as a proxy administrator for administrating said at least one smart card by transmitting at least authorization information from the remote administrator to the local administrator.

Claim 2 (original): A method according to claim 1 and wherein said establishing step is performed via said at least one user unit.

Claim 3 (original): A method according to claim 1 and wherein said establishing step comprises employing Internet Protocol (IP) for communication via the communication network.

Claim 4 (cancelled)

Claim 5 (original): A method according to claim 1 and also comprising the step of administrating said at least one smart card after communication with the remote administrator is established.

Claim 6 (original): A method according to claim 5 and wherein said administrating step comprises the step of administrating said at least one smart card immediately after communication with the remote administrator is established.

Claim 7 (previously amended): A method according to claim 4 and also comprising the step of administrating said at least one smart card after communication with the proxy administrator is established.

B1

Claim 8 (original): A method according to claim 7 and wherein said administrating step comprises the step of administrating said at least one smart card immediately after communication with the proxy administrator is established.

Claim 9 (original): A method according to claim 5 and wherein said administrating step comprises performing an administration initialization procedure to at least one of authenticate, verify and validate said at least one smart card.

Claim 10 (original): A method according to claim 9 and also comprising the step of preventing performance of any operation other than the administration initialization procedure until said administration initialization procedure is verified to be in order.

Claim 11 (original): A method according to claim 1 and wherein said step of employing the administrator identification information to identify the remote administrator comprises the step of identifying the at least one smart card in a smart card data base at the remote administrator.

Claim 12 (original): A method according to claim 1 and also comprising the step of accessing a protected information resource by said at least one smart card via the remote administrator associated therewith.

Claim 13 (original): A method according to claim 12 and wherein said accessing step comprises performing at least one administration operation.

Claim 14 (original): A method according to claim 13 and wherein said at least one administration operation comprises at least one of the following: transmission of a certificate; transmission of credentials; transmission of a key; renewal of said at least one smart card; expiration date updating; renewal of an authorization to said at least one smart card; validity check of data in said at least one smart card; integrity check of data in said at least one smart card; memory load/check; revocation of at least one of an authorization, a certificate and a smart card; execution of a "KILL CARD" process after a verification of a need to prevent operation of said at least one smart card; data load; and transmission of smart card chaining information.

B1

Claim 15 (original): A method according to claim 12 and wherein said accessing step comprises the step of performing security mechanisms for accessing the protected information resource by said at least one smart card.

Claim 16 (original): A method according to claim 15 and wherein said security mechanisms include at least one of the following: unilateral or bilateral authentication; time stamping; non-repudiation; digital signatures; distribution of an encryption key; change of an encryption key; encryption; and password authorization.

Claim 17 (original): A method according to claim 12 and wherein each operation performed during said accessing step by at least one of said remote administrator and said at least one smart card is performed only upon receipt of an "END

ADMINISTRATION OPERATION" instruction at a corresponding one of said at least one of said remote administrator and said at least one smart card.

Claim 18 (previously amended): A method according to claim 12 and wherein said remote administrator comprises a plurality of administrators, each operative to perform at least one of the following: at least part of said step of accessing the protected information resource; and at least part of an administration initialization procedure.

Claim 19 (original): A method according to claim 1 and wherein said communication network comprises at least one of the following: a local-area-network (LAN); a metropolitan-area-network (MAN); and a wide-area-network (WAN).

Claims 20 - 32 (canceled)

Claim 33 (currently amended): A system for remote administration of at least one smart card via a communication network, the system comprising:

a remote administrator having administrator identification information;

at least one user unit; and

at least one smart card associated with said remote administrator by storing in the at least one smart card said administrator identification information of the remote administrator, wherein

said at least one smart card inserted in said at least one user unit is operative to employ the administrator identification information to identify the remote administrator associated with said at least one smart card, and to establish communication via the communication network between the at least one smart card and the remote administrator in accordance with the administrator identification information,

and said communication is established by performing the following:

identifying a local administrator other than the remote administrator, the local administrator being positioned in the communication network in proximity to said at least one user unit; and

determining the local administrator as a proxy administrator for administrating said at least one smart card by transmitting at least authorization information from the remote administrator to the local administrator.

Claim 34 (canceled)

Claim 35 (previously presented): The system according to claim 33 and also comprising a smart card data base associated with the remote administrator, the smart card data base comprising information enabling identification of the at least one smart card.

B1

Claim 36 (previously presented): The system according to claim 33 and also comprising a protected information resource accessible by the at least one smart card via the remote administrator associated with the at least one smart card.

Claim 37 (previously presented): The system according to claim 36 and wherein the remote administrator comprises a plurality of administrators, each operative to perform at least one of the following: at least partially accessing the protected information resource; and at least part of an administration initialization procedure.

Claim 38 (currently amended): A system for remote administration of at least one smart card via a communication network, the system comprising:

means for associating said at least one smart card with a remote administrator by storing administrator identification information of the remote administrator in said at least one smart card;

means for inserting said at least one smart card in at least one user unit;

means for employing the administrator identification information stored in said at least one smart card to identify the remote administrator associated with said at least one smart card; and

means for establishing communication between the at least one smart card and the remote administrator via the communication network in accordance with the administrator identification information,

wherein said means for establishing comprises:

means for identifying a local administrator other than the remote administrator, the local administrator being positioned in the communication network in proximity to said at least one user unit; and

means for determining the local administrator as a proxy administrator for administrating said at least one smart card by transmitting at least authorization information from the remote administrator to the local administrator.

B1

Claim 39 (previously presented): The system according to claim 38 and wherein said means for employing the administrator identification information comprise means for identifying the at least one smart card in a smart card data base associated with the remote administrator.

Claim 40 (previously presented): The system according to claim 38 and also comprising means for accessing a protected information resource by said at least one smart card via the remote administrator associated with the at least one smart card.

Claim 41 (previously presented): The system according to claim 40 and wherein the remote administrator comprises a plurality of administrator means, each for performing at least one of the following: at least partially accessing the protected information resource; and at least part of an administration initialization procedure.

Claim 42 (new): The method according to claim 9 and wherein said administration initialization procedure comprises at least one of:

challenge-response of information related to shared secrets; and

challenge-response of information related to private keys.

B1

Claim 43 (new): A method according to claim 16 and wherein said unilateral or bilateral authentication comprise at least one of:

challenge-response of information related to shared secrets; and

challenge-response of information related to private keys.